

# Fraction-free algorithm for the computation of diagonal forms matrices over Ore domains using Gröbner bases

Viktor Levandovskyy<sup>1</sup>

*Lehrstuhl D für Mathematik, RWTH Aachen, Templergraben 64, 52062 Aachen, Germany*

Kristina Schindelar

*Siemens AG, Corporate Technology, Corporate Research and Technologies, Otto-Hahn-Ring 6, 81739 München, Germany*

---

## Abstract

This paper is a sequel to “Computing diagonal form and Jacobson normal form of a matrix using Gröbner bases” (Levandovskyy and Schindelar, 2011). We present a new fraction-free algorithm for the computation of a diagonal form of a matrix over a certain non-commutative Euclidean domain over a computable field with the help of Gröbner bases. This algorithm is formulated in a general constructive framework of non-commutative Ore localizations of  $G$ -algebras (OLGAs). We use the splitting of the computation of a normal form for matrices over Ore localizations into the diagonalization and the normalization processes. Both of them can be made fraction-free. For a given matrix  $M$  over an OLGA  $R$  we provide a diagonalization algorithm to compute  $U, V$  and  $D$  with fraction-free entries such that  $UMV = D$  holds and  $D$  is diagonal. The fraction-free approach allows to obtain more information on the associated system of linear functional equations and its solutions, than the classical setup of an operator algebra with coefficients in rational functions. In particular, one can handle distributional solutions together with, say, meromorphic ones. We investigate Ore localizations of common operator algebras over  $K[x]$  and use them in the unimodularity analysis of transformation matrices  $U, V$ . In turn, this allows to lift the isomorphism of modules over an OLGA Euclidean domain to a smaller polynomial subring of it. We discuss the relation of this lifting with the solutions of the original system of equations. Moreover, we prove some new results concerning normal forms of matrices over non-simple domains. Our implementation in the computer algebra system SINGULAR:PLURAL follows the fraction-free strategy and shows impressive performance, compared with methods which directly use fractions. In particular, we experience moderate swell of coefficients and obtain simple transformation matrices. Thus the method we propose is well suited for solving nontrivial practical problems.

---

<sup>1</sup> Corresponding author. Tel. +49 241 80 94546, Fax +49 241 80 92108

## Contents

1	Introduction	2
2	OLGAs and their Properties	3
2.1	Notations	4
3	Fraction-free or Polynomial Strategy	5
4	Solving Systems of Operator Equations	11
4.1	Ore Multiplicative Closure	12
4.2	Ore Closure in Classical Algebras	12
4.3	$\mathcal{F}$ is an $R$ -module	14
4.4	$\mathcal{F}$ is an $R_*$ -module	14
5	Cyclic Vector Method	15
6	Normal Form over a General Domain	17
7	Implementation and Examples	19
7.1	Comparison	19
7.2	Examples	19
8	Conclusion, Further Research and Open Problems	21
8.1	Further Research	21
8.2	Open Problems	22
9	Appendix. The Code for an Example	24

We know what we are, but know not  
what we may be.

---

William Shakespeare, “Hamlet”.

## 1. Introduction

This paper is a natural extension of our paper (Levandovskyy and Schindelar, 2011). We focus on the algorithmic computation of a diagonal form of a given matrix with entries in a Euclidean Ore algebra  $A$ . In contrast to commutative principal ideal domains ( $\mathbb{Z}$  or  $K[x]$  for a field  $K$ ), there is no such strong normal form as the Smith normal form. However, in the case when  $A$  is a simple algebra, there is a celebrated Jacobson normal form (Jacobson, 1943; Cohn, 1971) of remarkable structure. The existing proofs of diagonal and Jacobson normal forms offer an algorithm directly. However, such direct algorithms are rarely efficient in general.

We proposed the splitting of the computation of a normal form (like Jacobson form over simple domain) for matrices over Ore localizations into the *diagonalization* and the *normalization* processes. The diagonalization process can be formulated and applied in a fairly general setting, while the normalization depends on the algebra and on the properties of concretely given diagonal elements. Both diagonalization and normalization can be performed in a fraction-free fashion, and of course, the same ideas apply to the computation of the Smith normal form over a commutative Euclidean domain. As we demonstrate in Section 6, the question of normal forms over non-simple domains is widely open and distinctly differs from the case where Jacobson form exists.

---

Email addresses: [Viktor.Levandovskyy@math.rwth-aachen.de](mailto:Viktor.Levandovskyy@math.rwth-aachen.de) (Viktor Levandovskyy),  
[kristina.schindelar@siemens.com](mailto:kristina.schindelar@siemens.com) (Kristina Schindelar).

In this paper we concentrate on the diagonalization and present the fraction-free Algorithm 3.12, which is based on Gröbner bases, and its implementation in SINGULAR:PLURAL Greuel et al. (2010). As a byproduct, we obtain a fraction-free algorithm for the computation of the Smith normal form over a commutative Euclidean domain.

Many operator algebras are non-commutative skew polynomial rings (Kredel, 1993; Chyzak and Salvy, 1998; Bueso et al., 2003; Levandovskyy, 2005; Chyzak et al., 2007). We propose a new class of univariate skew polynomial rings, which are obtained as Ore localizations of  $G$ -algebras (OLGAs, see Def. 2.2). This framework is powerful, convenient and constructive at the same time. Notably, it is possible to perform algorithmic computations like Gröbner bases for modules in such algebras. Moreover, many computations can be done in a fraction-free manner and hence they can be implemented in any computer algebra system, which can handle  $G$ -algebras or general polynomial Ore algebras.

Such algebras allow to describe time varying systems in systems and control theory (Zerz, 2007), (Ilchmann and Mehrmann, 2006), (Ilchmann et al., 1984) and constitute a general framework for dealing with linear operator equations with variable coefficients. In (Culianez and Quadrat, 2005), applications of a Jacobson form to systems of partial differential equations are shown and several concrete examples are introduced.

In Section 4 we discuss solutions to a given system of operator equations with variable coefficients. Starting with a polynomial ring  $R_*$  and its 'big' localization  $R$ , we denote by  $M$  the presentation matrix  $R_*$ -module, corresponding to the system of equations. We compute matrices  $U, V$  and a diagonal matrix  $D$ , such that  $UMV = D$ . Then, we determine a smaller localization  $R' \subset R$  of  $R_*$ , over which both  $U, V$  become invertible. We provide a module isomorphism for  $R'$ -modules, which allows to treat more general solutions, than those one can obtain with the  $R$ -module structure.

In Prop. 5.1 we propose an algorithm for a probabilistic computation of a Jacobson form via a cyclic vector. Moreover, we provide both experimental data from computations and analysis of this data.

At the end, we pose five open problems. In the Appendix, we put the detailed explanation on the usage of our implementation.

## 2. OLGAs and their Properties

By  $K$  we denote a computable field. Describing associative  $K$ -algebras via finite sets of generators  $G$  and relations  $R$ , one usually writes  $A = K\langle G \mid R \rangle = K\langle G \rangle / \langle R \rangle$ . It means that  $A$  is a factor algebra of the free associative algebra  $K\langle G \rangle$  modulo the two-sided ideal, generated by  $R$ . Recall the following definition.

**Definition 2.1.** Let  $A$  be a quotient of the free associative algebra  $K\langle x_1, \dots, x_n \rangle$  by the two-sided ideal  $I$ , generated by the finite set  $\{x_j x_i - c_{ij} x_i x_j - d_{ij}\}$  for all  $1 \leq i < j \leq n$ , where  $c_{ij} \in K^*$  and  $d_{ij}$  are polynomials<sup>2</sup> in  $x_1, \dots, x_n$ . Then  $A$  is called a  $G$ -algebra (Levandovskyy and Schönemann, 2003; Levandovskyy, 2005), if

- for all  $1 \leq i < j < k \leq n$  the expression  $c_{ik} c_{jk} \cdot d_{ij} x_k - x_k d_{ij} + c_{jk} \cdot x_j d_{ik} - c_{ij} \cdot d_{ik} x_j + d_{jk} x_i - c_{ij} c_{ik} \cdot x_i d_{jk}$  reduces to zero modulo  $I$  and

<sup>2</sup> Without loss of generality (cf. (Levandovskyy, 2005)) we can assume that  $d_{ij}$  are given in terms of standard monomials  $x_1^{a_1} \dots x_n^{a_n}$

- there exists a monomial ordering  $\prec$  on  $K[x_1, \dots, x_n]$ , such that for each  $i < j$  with  $d_{ij} \neq 0$ ,  $\text{lm}(d_{ij}) \prec x_i x_j$ . Here,  $\text{lm}$  stands for the classical notion of leading monomial of a polynomial from  $K[x_1, \dots, x_n]$ .

A monomial ordering on  $K[x_1, \dots, x_n]$  carries over to a  $G$ -algebra (and is called **admissible**) as in the definition as soon as it satisfies the second condition of the definition.

As in Levandovskyy and Schindelar (2011), we continue working with Ore localizations of  $G$ -algebras, which are principal ideal domains. A  $G$ -algebra  $R$  is a Noetherian integral domain, hence there exists its total two-sided ring of fractions  $\text{Quot}(R) = (R \setminus \{0\})^{-1}R$ , which is a division ring (skew field). It is convenient to define a class of subalgebras between  $R$  and  $\text{Quot}(R)$  as follows.

**Definition 2.2.** Let  $R$  be a  $G$ -algebra, generated by the set  $X = \{x_1, \dots, x_{n+1}\}$ . Suppose, that there is a  $m$  with  $1 \leq m \leq n$  and a subset  $Y = \{x_{i_1}, \dots, x_{i_m}\}$ , such that  $d_{i_j, i_k}$  does not involve other variables than those from  $Y$ . Then  $B := K\langle Y \mid \{x_j x_i - c_{ij} x_i x_j - d_{ij} \mid i < j, x_i, x_j \in Y\} \rangle$  is a  $G$ -algebra. For a proper completely prime ideal  $I \subset B$ ,  $B/I$  is a domain. If, in addition,  $S := (B/I) \setminus \{0\}$ <sup>3</sup> is an Ore set in  $A$ , then we call  $S^{-1}R$  an OLGA (Ore-localized  $G$ -algebra). It is encoded via the triple  $(R, B, I)$ .

From now on (for simplicity) we consider only OLGAs of the form  $(R, B, 0)$ .

Prop. 28 of (García García et al., 2009) implies the following characterization of OLGAs. Let  $Z = X \setminus Y$  in the notations as in the above definition. If there exists an admissible  $(Y, Z)$ -block ordering on  $R$ , then  $B \setminus \{0\}$  is an Ore set in  $R$ .

If we put  $m = n$  in Definition 2.2, a corresponding OLGA is a Euclidean domain, which we then shorten as OLGAED. Let  $X \setminus Y = \{d\}$ . In Levandovskyy and Schindelar (2011), we proved in Theorem 2.6, that for the case of OLGAED it is enough to require the existence of an admissible ordering on  $A$ , which satisfies  $d > x_{i_j}$  for all  $1 \leq j \leq n$ . Moreover, the OLGAED  $(B \setminus \{0\})^{-1}R$  can be presented as an Ore extension of  $\text{Quot}(B)$  by the variable  $d$ .

### 2.1. Notations

In what follows we will work with OLGAED, given as Ore extension  $R = A[d; \sigma, \delta]$ , where  $A = \text{Quot}(A_*)$  and  $A_*$  is a  $G$ -algebra in variables  $\{x_1, \dots, x_n\}$ . The computations will be performed in a  $G$ -algebra  $R_* = A_*[d; \sigma, \delta]$ <sup>4</sup> with respect to the monomial module ordering POT (position-over-term), defined as follows. For  $r, s \in \text{Mon}(R_*)$  and the canonical basis  $\{e_k\}$  of a free module of finite rank,

$$re_i < se_j \Leftrightarrow i < j \text{ OR } (i = j \text{ and } r < s),$$

and  $r < s$  with respect to an admissible well-ordering on  $R_*$ , in which  $d$  is bigger than any monomial not involving  $d$ . In  $R$ , a Gröbner basis is computed with respect to the induced POT ordering.

<sup>3</sup> Note, that  $I$  is an ideal in  $B$  and may not be an ideal in  $R$ . Moreover, elements of  $S$  are identified with residue classes modulo  $I$ .

<sup>4</sup> Note, that  $A_* \subset A \subset R$  and  $A_* \subset R_* \subset R$ .

### 3. Fraction-free or Polynomial Strategy

Suppose a matrix  $M$  over a non-commutative Euclidean domain  $R$  is given. Without loss of generality, we suppose that  $M$  does not contain a zero row. In this section, we show our main approach of this paper. We introduce a method that allows to execute Algorithm 3.5 from Levandovskyy and Schindelar (2011) in a completely fraction-free framework. The idea comes from commutative algebra (see e. g. (Gianni et al., 1988)). Gröbner bases were used for the computation of commutative Smith forms in e. g. (Insua, 2005).

We define the **degree** of an element in  $R_*$  to be the weighted degree function with weight 0 to any generator of  $A_*$  and weight 1 to  $\partial$ . Thus this weighted degree of  $f \in R_*$  coincides with the degree of  $f$  in  $R$  and it is invariant under the multiplication by nonzero elements in  $A_*$ .

**Lemma 3.1.** Let  $M \in R^{p \times q}$ . Then there exists a diagonal  $R$ -unimodular matrix  $T \in A_*^{p \times p}$  such that  $TM \in R_*^{p \times q}$ . Moreover, the computation of such  $T$  is algorithmic.

*Proof.* If  $M \in R_*^{p \times q}$ , there is nothing to do. Suppose that  $M$  contains elements with fractions. At first, we show how to bring two fractional elements  $a^{-1}b, c^{-1}d$  for  $a, c \in A_*$ ,  $b, d \in R_*$  to a common left denominator, cf. (Apel, 1988). For any  $h_1, h_2 \in A_*$ , such that  $h_1a = h_2c$ , it is easy to see that

$$(h_1a)^{-1}(h_1b) = a^{-1}h_1^{-1}h_1b = a^{-1}b \text{ and } (h_1a)^{-1}(h_2d) = (h_2c)^{-1}(h_2d) = c^{-1}d,$$

hence  $(h_1a)^{-1} = a^{-1}h_1^{-1} = (h_2c)^{-1}$  is a common left denominator. Analogously we can compute a common left denominator for any finite set of fractions. Let  $T_{ii}$  be a common left denominator of all non-zero elements in the  $i$ -th row of  $M$ , then  $TM$  contains no fractions. Moreover,  $T$  is a diagonal matrix with non-zero entries from  $A_*$ , hence it is  $R$ -unimodular.  $\square$

**Remark 3.2.** Note that the computation of compatible factors  $h_i$  for  $a_1, a_2 \in A_*$  can be achieved by computing syzygies, since  $\{(h_1, h_2) \in A_*^2 \mid h_1a_1 = h_2a_2\}$  is precisely the module  $\text{Syz}(a_1, -a_2) \subset A_*^2$ . The factors  $h_i$  for more  $a_i$ 's can be obtained as well.

**Notation.** By  $\mathcal{G}(R_* M_*)$  we denote the reduced left Gröbner basis of the submodule  $R_* M_*$  with respect to the module ordering  $<_*$  on  $R_*$ , defined in (2.1). Note, that monomials of  $R_*^{1 \times q}$  are of the form  $x_1^{\alpha_1} \cdots x_n^{\alpha_n} \partial^\beta e_k$  for  $\alpha_i, \beta \in \mathbb{N}$ ,  $1 \leq k \leq q$  and  $e_k$  is the  $k$ -th canonical basis vector. Let  $m$  be a nonzero vector with entries in  $R_*$ . Then by  $\text{lm}(m)$  we denote the leading monomial of  $m$  with respect to  $<_*$  and by  $\text{lpos}(m) = k$  the leading position of  $\text{lm}(m)$ . By  $\deg(m)$  we denote  $\deg(\text{lm}(m)) = \deg(x_1^{\alpha_1} \cdots x_n^{\alpha_n} \partial^\beta e_k) = \beta$ .

For  $M \in R^{p \times q}$ , we denote by  ${}_R M = R^{1 \times p} M$  the left  $R$ -module, generated by the rows of  $M$ .

Define  $M_* := TM \in R_*^{p \times q}$  using the notation of Lemma 3.1. Then the relations  ${}_R M_* \subseteq {}_R M$  and  ${}_R M_* = {}_R M$  hold obviously. Thus whenever we speak about a finitely generated submodule  ${}_R M \subset R^{1 \times q}$ , we denote by  ${}_R M_*$  a presentation of  ${}_R M$  with generators contained in  $R_*$ . In what follows, we will show how to find  $R$ -unimodular matrices

$U \in R_*^{p \times p}$  and  $V \in R_*^{q \times q}$  such that

$$U(TM)V = \begin{bmatrix} r_1 & & & \\ & \ddots & & \\ & & r_q & \\ & & & 0 \end{bmatrix} \in R_*^{p \times q}.$$

Since  $U(TM)V = (UT)MV$  and  $UT$  is a  $R$ -unimodular matrix, our initial aim follows.

**Remark 3.3.** Using the fraction-free strategy, two improvements can be observed. On the one hand, once we have mapped the matrix we work with from  $R^{p \times q}$  to  $R_*^{p \times q}$ , the complicated arithmetics in the skew field of fractions is not used anymore. The other improvement lies in the nature of the construction of normal forms for matrices and the corresponding transformation matrices. The naive approach would be to apply elementary operations inclusive division by invertibles on the rows and columns, that is, operations from the left and from the right. Indeed, there are methods using different techniques like, for instance,  $p$ -adic arguments to calculate the invariant factors of the Smith form over  $\mathbb{Z}$  (Lübeck, 2002), but this method does not help in constructing transformation matrices. Surely the swap from left to right has no influence in the commutative framework. But already in the rational Weyl algebra  $B_1$ ,  $\frac{1}{x}$  is an unit in  $B_1$  and  $\partial \frac{1}{x} = \frac{1}{x} \partial - \frac{1}{x^2}$ . Comparing the multiplication by the inverse element, that is, with  $x$ , we see that  $\partial x = x \partial + 1$  holds. Thus a multiplication of any polynomial containing  $d$  with the element  $\frac{1}{x}$  in the field of fractions causes an immediate coefficient swell. Since a normal form of a matrix is given modulo unimodular operations, the previous example illustrates the variations of possible representations. In examples, which we gather in the Subsection 7.2, the fraction-free strategy leads to a moderate increase of coefficients.

On the other hand, switching to the polynomial framework changes the setup. The algebra  $R_*$  is not a principal ideal domain anymore, which was the essential property for the existence of a diagonal form over  $R$ . In the sequel, we show how that this problem can be resolved by introducing a suitable sorting condition for the chosen module ordering. Referring to the argumentation of Lemma 3.5 yields the block-diagonal form 1 with the 0 block above.

$$\mathcal{G}_{(R_*M_*)} = \begin{bmatrix} 0 & \dots & \dots & 0 \\ \boxed{*} & & & \\ \vdots & & 0 & \\ * & \boxed{*} & & \\ & \vdots & 0 & \\ & * & & \\ & & \ddots & \\ & & & \boxed{*} \\ & & & \vdots \\ & * & & * \end{bmatrix}. \quad (1)$$

Moreover, the rows with the boxed element have the smallest leading monomial with respect to the chosen ordering in the corresponding block. A block denotes all elements of the same leading position in  $\mathcal{G}_{(R_*M_*)}$ . In Theorem 3.9 we show that these elements indeed generate  ${}_R M$ , while in Lemma 3.7 we show that these elements provide us with additional information. However, this result requires some preparations.

**Lemma 3.4.** Let  $P$  be  $R$  or  $R_*$ . For  $M \in P^{p \times q}$  of full rank and for every  $1 \leq i \leq q$ , define  $\alpha_i := \min\{\deg(a) \mid a \in {}_P M \setminus \{0\} \text{ and } \text{lpos}(a) = i\}$ . Then for all  $1 \leq i \leq q$ , there exists  $h_i \in \mathcal{G}({}_P M)$  of degree  $\alpha_i$  with  $\text{lpos}(h_i) = i$ .

*Proof.* Recall that with respect to  $<_*$ ,  $d$  is bigger than any monomial not involving  $d$ . Let  $f \in {}_P M$  with  $\text{lpos}(f) = i$  and  $\deg(f) = \alpha_i$ . Suppose that for all  $g \in \mathcal{G}({}_P M)$  with leading position  $i$ ,  $\deg(g) > \alpha_i$  holds. Since  $\mathcal{G}({}_P M)$  is a Gröbner basis, there exists  $g \in \mathcal{G}({}_P M)$  such that  $\text{lm}(g)$  divides  $\text{lm}(f)$ . This happens if and only if  $\deg(g) \leq \deg(f)$  (because  $R_*$  is a  $G$ -algebra and  $R$  is an OLGAED), which yields a contradiction.  $\square$

The full rank assumption in the lemma guarantees the existence of  $\alpha_i$  for each component  $1 \leq i \leq q$ . Note, that over  $P = R_*$  the cardinality of  $\{\deg(a) \mid a \in {}_P M \setminus \{0\} \text{ and } \text{lpos}(a) = i\}$  is greater than one in general, hence there might be different selection strategies. We propose to select an element according to  $\min_{<_*}$ , see Lemma 3.7. Recall the Lemma 3.3. from (Levandovskyy and Schindelar, 2011):

**Lemma 3.5.** If one orders a reduced Gröbner basis in such a way, that  $\text{lm}(\mathcal{G}({}_R M)_1) < \dots < \text{lm}(\mathcal{G}({}_R M)_m)$ , then  $[\mathcal{G}({}_R M)_1, \dots, \mathcal{G}({}_R M)_m]^T$  is a lower triangular matrix.

**Corollary 3.6.** Lemma 3.4 and Lemma 3.5 yield

$$\deg(\mathcal{G}({}_R M)_i) = \min\{\deg(a) \mid a \in {}_R M \setminus \{0\} \text{ and } \text{lpos}(a) = i\}.$$

**Lemma 3.7.** Let  $\alpha_i$  be the degree of the boxed entry with leading position in the  $i$ -th column, that is

$$\alpha_i := \deg(\min_{<_*} \{\text{lm}(b) \mid b \in \mathcal{G}(R_* M_*) \text{ and } \text{lpos}(b) = i\}).$$

Then for all  $h \in {}_R M$  with  $\text{lpos}(h) = i$  we have  $\deg(\text{lm}(h)) \geq \alpha_i$ .

*Proof.* Suppose that the claim does not hold and there is  $h \in {}_R M$  with  $\text{lpos}(h) = i$  of degree smaller than  $\alpha_i$ . By Lemma 3.1, there exists  $a \in A_*$  such that  $ah \in {}_{R_*} M_*$ . Then  $\deg(ah) = \deg(h)$  and  $\text{lpos}(ah) = i$ . Due to Lemma 3.4,  $\deg(f) \geq \alpha_i$  for all  $f \in {}_{R_*} M_*$  with leading position  $i$ , hence we obtain a contradiction.  $\square$

**Corollary 3.8.** Lemma 3.7 and Corollary 3.6 imply, that for all  $1 \leq i \leq q$

$$\min\{\deg(a) \mid a \in {}_R M \setminus \{0\} \wedge \text{lpos}(a) = i\} = \min\{\deg(a) \mid a \in {}_{R_*} M_* \setminus \{0\} \wedge \text{lpos}(a) = i\}.$$

**Theorem 3.9.** Let  $M \in R^{p \times p}$  be of full rank. For each  $1 \leq i \leq p$ , let  $\alpha_i$  be as in Lemma 3.7. Let us define  $b_i$  to be the element from  $\{b \in \mathcal{G}({}_{R_*} M_*) : \text{lpos}(b) = i, \deg(b) = \alpha_i\}$  with the smallest leading monomial. Then  ${}_R \langle b_1, \dots, b_p \rangle = {}_R M$ . Moreover, the set  $\{b_1, \dots, b_p\}$  corresponds to the subset of all rows with a boxed entry in the block triangular form 1.

*Proof.* Since  $M$  is of full rank, the minimum in the definition of  $b_i$  exists for each  $1 \leq i \leq p$ . Let  $f \in {}_R M \setminus \{0\}$ . Due to Corollary 3.8, there exists  $1 \leq k \leq p$  such that  $\text{lpos}(b_k) = \text{lpos}(f)$  and  $\deg(b_k) \leq \deg(f)$ . Thus there exists an element  $s_k \in R$  such that  $\deg(f - s_k b_k) < \deg(b_k)$ . Since  $f - s_k b_k \in {}_R M$ , Corollary 3.8 implies that we have  $\text{lpos}(f - s_k b_k) < \text{lpos}(f)$ . Iterating this reduction leads to the remainder zero and thus  $f = \sum_{i=1}^k s_i b_i$ .  $\square$

**Notation.** Using the notation of the previous theorem, let  $\mathcal{G}^*({}_R M) := [b_1, \dots, b_p]^T$ , which is by construction a lower triangular matrix. In the sequel, let  $M \in R^{p \times p}$  be of full rank. Then  $\mathcal{G}^*({}_R M)$  is a square matrix.

Recall that an involutive anti-automorphism (or an **involution**)  $\theta$  of a ring  $A$  is a  $K$ -linear map, satisfying  $\theta(ab) = \theta(b)\theta(a)$  for all  $a, b \in A$  and  $\theta^2 = \text{id}_A$ . Moreover, we define by  $\tilde{\theta}(M)$  the application of an involution  $\theta$  to the entries of the transpose of  $M$ .

**Proposition 3.10.** Suppose  $M \in R^{p \times p}$  is a full rank matrix and there is  $U_* \in R_*^{\ell \times p}$  such that  $U_* M_* = \mathcal{G}({}_{R_*} M_*)$ . Let us select the indices

$$\{t_1, \dots, t_p\} \subseteq \{1, \dots, \ell\} \text{ such that } \{(U_* M_*)_{t_1}, \dots, (U_* M_*)_{t_p}\} = \mathcal{G}^*({}_R M) \quad (2)$$

Then  $U := [(U_*)_{t_1}, \dots, (U_*)_{t_p}]^T$  is  $R$ -unimodular in  $R^{p \times p}$  and  $U M_* = \mathcal{G}^*({}_R M)$ .

*Proof.* The equality  $U M_* = \mathcal{G}^*({}_R M)$  follows by the definition of  $U$ . Now we show that  $U$  is  $R$ -unimodular. Note that  $U M_* \subset R^{p \times p} \supset M_*$  and  ${}_R(U M_*) = {}_R \mathcal{G}^*({}_R M) = {}_R M = {}_R M_*$  holds. Thus there exists  $V \in R^{p \times p}$  such that  $M_* = V(U M_*)$ . Then  $VU = \text{id}_{p \times p}$  and analogously  $UV = \text{id}_{p \times p}$  since  $M$  has full row rank.  $\square$

**Lemma 3.11.** The equality of the following left ideals holds:

$${}_R \langle \theta(\mathcal{G}^*({}_R M)_{p1}), \dots, \theta(\mathcal{G}^*({}_R M)_{pp}) \rangle = {}_R \langle \mathcal{G}^*(\tilde{\theta}(\mathcal{G}^*({}_R M)))_{pp} \rangle.$$



*Proof.* Using the argumentation given in the proof of Lemma 3.4. of (Levandovskyy and Schindelar, 2011), we obtain

$${}_R\langle\theta(\mathcal{G}^*({}_RM)_{p1}), \dots, \theta(\mathcal{G}^*({}_RM)_{pp})\rangle = {}_R\langle\mathcal{G}(\tilde{\theta}(\mathcal{G}^*({}_RM)))_{pp}\rangle.$$

Because of  ${}_R\mathcal{G}^*({}_RM) = {}_R\mathcal{G}({}_RM)$  we have  $\tilde{\theta}(\mathcal{G}^*({}_RM))_R = \tilde{\theta}(\mathcal{G}({}_RM))_R$  and thus  ${}_R\mathcal{G}^*(\tilde{\theta}(\mathcal{G}^*({}_RM))) = {}_R\mathcal{G}(\tilde{\theta}(\mathcal{G}({}_RM)))$ . Since both  $\mathcal{G}(\tilde{\theta}(\mathcal{G}({}_RM)))$  and  $G^*(\tilde{\theta}(\mathcal{G}^*({}_RM)))$  are lower triangular matrices, with the latter identity above we obtain  ${}_R\langle\mathcal{G}(\tilde{\theta}(\mathcal{G}({}_RM)))_{pp}\rangle = {}_R\langle\mathcal{G}^*(\tilde{\theta}(G^*({}_RM)))_{pp}\rangle$ .  $\square$

Now we are ready to formulate the fraction-free version of the Algorithm 3.5 *Diagonalization with Gröbner bases* from (Levandovskyy and Schindelar, 2011).

**Algorithm 3.12** (Fraction-free diagonalization with Gröbner Bases).

**Input:**  $M \in R^{p \times p}$  of full rank,  $\theta$  an involution on  $R_*$  and  $\tilde{\theta}$  as above.

**Output:**  $R$ -unimodular matrices  $U, V, D \in R_*^{p \times p}$  such that  $U \cdot M \cdot V = D = \text{Diag}(r_1, \dots, r_p)$ .

Find  $T \in R^{p \times p}$  unimodular such that  $TM \in R_*^{p \times p}$

$M^{(0)} \leftarrow TM, \quad U \leftarrow T, \quad V \leftarrow \text{id}_{p \times p}$

$i \leftarrow 0$

**while**  $M^{(i)}$  is not a diagonal matrix **or**  $i \equiv_2 1$  **do**

$i \leftarrow i + 1$

Compute  $U^{(i)}$  so that  $U^{(i)} \cdot M^{(i-1)} = \mathcal{G}({}_{R_*}M^{(i-1)}) \in R_*^{\ell \times p}$

Select  $\{t_1, \dots, t_p\} \subseteq \{1, \dots, \ell\}$  as in (2) of Prop. 3.10

$U^{(i)} \leftarrow [(U^{(i)})_{t_1}, \dots, (U^{(i)})_{t_p}]^T$

$M^{(i)} \leftarrow \tilde{\theta}(G^*({}_RM))$

**if**  $i \equiv_2 0$  **then**

$V \leftarrow V \cdot \tilde{\theta}(U^{(i)})$

**else**

$U \leftarrow U^{(i)} \cdot U$

**end if**

**end while**

**return**  $(U, V, M^{(i)})$

**Remark 3.13.** It is important to mention, that the matrices  $U, V, D$  (hence the elements  $r_i$  as well) have entries from  $R_*$ , that is, they are polynomials. However,  $U$  and  $V$  are only unimodular over  $R$  and, in general, they need not be unimodular over  $R_*$  for obvious reasons. In Subsection 7.2 we will investigate, over which subalgebras of  $R$  the matrices  $U$  or  $V$  become unimodular.

**Theorem 3.14.** Algorithm 3.12 terminates with the correct result.

*Proof.* The proof is a natural generalization of the proof of the Theorem 3.6. from (Levandovskyy and Schindelar, 2011). At first, we use Proposition 3.10. Moreover, Lemma 3.11 provides a replacement for the arguments we used in the Lemma 3.4. of (Levandovskyy and Schindelar, 2011).  $\square$

Algorithm 3.12, as well as the original algorithm of (Levandovskyy and Schindelar, 2011), can be extended to  $M \in R^{p \times q}$  along the lines already discussed in Remark 3.7

of (Levandovskyy and Schindelar, 2011). Our implementation (cf. Section 7) works for arbitrary matrices.

As for examples, a  $2 \times 2$  matrix over the Weyl algebra has been considered in detail in Example 3.8 of (Levandovskyy and Schindelar, 2011). Note that a fraction-free method was used indeed.

**Example 3.15.** Consider the first shift algebra  $R_* = S_1 = K\langle x, s \mid sx = xs + s \rangle$  and its localization (often called the first rational shift algebra)  $R = K(x)\langle s \mid sx = xs + s \rangle$ . There are precisely two involutions, which can be presented by diagonal matrices on  $R_*$ , namely  $x \mapsto -x, s \mapsto -s$  and  $x \mapsto -x, s \mapsto s$ . Let us take the latter and call it  $\theta$ . Consider the matrix in  $R_*^{2 \times 3}$

$$M = \begin{bmatrix} (x-1)s + x^2 - x & xs + x^2 & (x+2)s + x^2 + 2x \\ s + x & 0 & s \end{bmatrix}.$$

As we can see,  $T = \text{id}_{2 \times 2}$  and thus  $M^{(0)} := M$ ,  $U = \text{id}_{2 \times 2}$ ,  $V = \text{id}_{3 \times 3}$  and  $i = 0$ . Since  $M$  is not a square matrix, under the *while* condition “while  $M^{(i)}$  is not a diagonal matrix” in the Algorithm we mean the following. The computation will run until the matrix we obtain contains a diagonal square submatrix and the entries outside of this submatrix are zero.

**1:** Since  $M^{(0)}$  is not diagonal, we enter the while loop.  $i := 1$ .

$$M' := \mathcal{G}_{(R_*)} M^{(0)} = \begin{bmatrix} -3s^2 - (x^2 + 7x + 6)s - x^3 - 4x^2 - 3x & (x+1)s^2 + (x^2 + 2x + 1)s & 0 \\ -3s - 3x & xs + x^2 & x^2 + 2x \end{bmatrix}$$

We set  $U := U_1$ , where  $U_1 M^{(0)} = M'$  and

$$U_1 = \begin{bmatrix} s & -(x+3)s - x^2 - 4x - 3 \\ 1 & -x - 2 \end{bmatrix}.$$

Moreover,  $M^{(1)} := \tilde{\theta}(M') \in R_*^{3 \times 2}$ .

**2:** Since  $M^{(1)}$  is not diagonal, we enter the while loop.  $i := 2$ .

$$M^{(1)} = \begin{bmatrix} -3s^2 - x^2s + 5xs + x^3 - 4x^2 + 3x & -3s + 3x \\ -xs^2 - s^2 + x^2s & -xs - s + x^2 \\ 0 & x^2 - 2x \end{bmatrix}$$

$$M' := \mathcal{G}_{(R_*)} M^{(1)} = \begin{bmatrix} 0 & 0 \\ 4x^4 + 12x^3 - 4x^2 - 12x & 0 \\ -4xs - 4s & -4x \end{bmatrix}$$

The transformation matrix  $U_2 \in R_*^{3 \times 3}$  is dense, so we show its highest terms with respect to  $s$ :

$$U_2 = \begin{bmatrix} -(x^2 + 5x - 6)s^2 + \dots & -7(x-1)s^2 + \dots & (-x+1)s^2 + \dots \\ -3(x+6)s^2 + \dots & -21s^2 + \dots & -3s^2 + \dots \\ (x^2 + 5x - 6)s^2 + \dots & 7(x-1)s^2 + \dots & (x-1)s^2 + \dots \end{bmatrix}$$

Moreover, we put  $M^{(2)} := \tilde{\theta}(M') \in R_*^{2 \times 3}$  and  $V := \tilde{\theta}(U_2)$ .

**3:** Since  $M^{(2)}$  is not diagonal, we enter the while loop.  $i := 3$ .

$$M^{(2)} = \begin{bmatrix} 0 & 4x^4 + 12x^3 - 4x^2 - 12x & -4xs - 4s \\ 0 & 0 & -4x \end{bmatrix}$$

$$M' := \mathcal{G}_{(R_*)} M^{(2)} = \begin{bmatrix} 0 & 4(x^4 + 3x^3 - x^2 - 3x) & 0 \\ 0 & 0 & 4x \end{bmatrix} = U_3 M^{(2)}, \text{ where } U_3 = \begin{bmatrix} 1 & -s \\ 0 & -1 \end{bmatrix}.$$

Thus we define  $M^{(3)} := \tilde{\theta}(M') \in R_*^{2 \times 3}$  and  $U := U_3 \cdot U$ .

**4:** Since  $M^{(3)}$  is diagonal (that is, consists of a diagonal submatrix and the rest of entries are zeros) but  $i = 1 \pmod 2$ , we do one more run, which finishes and returns the final data:

$$D = \begin{bmatrix} 0 & (x-1)x(x+1)(x+3) & 0 \\ 0 & 0 & x \end{bmatrix}, U = \frac{1}{4} \begin{bmatrix} 0 & -(x+1)(x+3) \\ 1 & -(x+2) \end{bmatrix}, V =$$

$$\begin{bmatrix} -(x^2 + 5x - 6)s^2 - (x^3 + 4x^2 - x - 4)s & -7(x-1)s^2 - (3x^2 + 5x - 8)s - 4x + 4 & v_{13} \\ -3(x+6)s^2 - (x^3 + 7x^2 + 5x - 13)s - x^4 - 2x^3 + 7x^2 + 8x - 12 & -21s^2 - (7x^2 + 2x - 11)s - 3x^3 - 2x^2 + 13x - 8 & v_{23} \\ (x^2 + 5x - 6)s^2 + (2x^3 + 6x^2 - 14x + 6)s + x^4 - 7x^2 + 6x & 7(x-1)s^2 + (10x^2 - 16x + 6)s + 3x^3 - 4x^2 - 5x + 6 & v_{33} \end{bmatrix},$$

where  $v_{13} = (x-1)s^2 + (x^2 - x)s$ ,  $v_{23} = 3s^2 + (x^2 + 2x - 5)s + x^3 - 2x^2 - 3x + 8$  and  $v_{33} = (-x+1)s^2 - 2(x-1)^2s - x^3 + 4x^2 - 5x + 2$ . Indeed, since both nonzero diagonal entries are units in  $K(x)$ , the output matrix can be further reduced to

$$D' = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

However, then one has to divide explicitly by polynomials in  $x$  in transformation matrices. We are not going to do this. Moreover, in what follows we will show, how to get important information from such matrices containing units from the non-constant ground field. As for the concrete example, we conclude, that  $R^3/R^2M \cong R$ , thus a system module of  $M$  is free of rank 1 over  $R$ .

#### 4. Solving Systems of Operator Equations

**Remark 4.1.** Let us settle the terminology. Let  $A$  be the  $K$ -algebra of  $K$ -linear operators. Consider a system of equations in unknown functions  $\omega_1, \dots, \omega_m$ . A system is linear, if it can be written in the matrix notation, that is  $S \cdot [\omega_1, \dots, \omega_m]^T = 0$ , where  $S$  is a rectangular matrix with entries from  $A$ . Then one associates to  $S$  a left  $A$ -module  $\mathcal{M}$ , which is finitely presented by the matrix  $S$ . Given a left  $A$ -module  $\mathcal{F}$ , we usually speak of *solutions of  $\mathcal{M}$  in  $\mathcal{F}$* . The celebrated Lemma of B. Malgrange tells us, that the solutions to a linear system of equations  $S$  in a left  $A$ -module  $\mathcal{F}$  are in one-to-one correspondence with the elements of the abelian group  $\text{Hom}_A(\mathcal{M}, \mathcal{F})$ . This allows us to

avoid the reference to a specific solution space by addressing an abstract one. However, in the context of this paper we address the space of distributions (though yet more general hyperfunctions fit into our framework as well) as the space of more general solutions in addition to meromorphic functions.

Assume there is a bigger function space  $\mathcal{G}$ , which is an  $A$ -module. Thus we have an exact sequence  $0 \rightarrow \mathcal{F} \rightarrow \mathcal{G}$ . Due to the left exactness of the Hom functor, we obtain that  $0 \rightarrow \text{Hom}_A(\mathcal{M}, \mathcal{F}) \rightarrow \text{Hom}_A(\mathcal{M}, \mathcal{G})$  is an exact sequence as well. This justifies the fact, that working with a more general solution space  $\mathcal{G}$  we obtain not less solutions to a module  $\mathcal{M}$  as with  $\mathcal{F}$ .

An  $R$ -module is naturally an  $R_*$ -module, but an  $R_*$ -module is not necessarily an  $R$ -module. There can be  $R_*$ -modules  $M$  with  $S$ -torsion, that is those for which  $S^{-1}M = 0$  holds. Hence, though working over  $R$  brings significant comfort, we are interested in gaining more information from the algebraic structure by looking at  $R_*$  and, more generally, subalgebras between  $R_*$  and  $R$ . Since there are  $R_*$ -modules, which are not  $R$ -modules, in view of Malgrange's Lemma there might be more solutions in  $R_*$ -modules as in  $R$ -modules. See Examples 4.9 and 4.10 for illustrative details.

We need to recall and develop mechanisms, which allow us to tackle localizations of operator algebras. We will show, how different small enough localizations look for common operator algebras.

#### 4.1. Ore Multiplicative Closure

Let  $W \in R^{r \times r}$  be a square matrix with entries in  $R$ . Assume that there exists left inverse matrix  $T$ , that is  $TW = \text{id}_{r \times r}$ . Then by Lemma 3.1 there exists a diagonal matrix  $Q = \text{Diag}(\dots, q_{ii}, \dots)$  such that  $Q$  (resp.  $QT$ ) has entries from  $A_*$  (resp.  $R_*$ ). Let  $\Omega = \{q_{ii} \mid 1 \leq i \leq r, q_{ii} \notin K\} \cup \{1\}$ . Denote by  $R_W$  the Ore localization of  $R_*$  with respect to a multiplicatively closed Ore set  $S_W$ , which is defined as follows. Let  $\mathcal{M}(\Omega)$  be the two-sided multiplicative closure of  $\Omega$ , equivalently the (possibly non-commutative) monoid, generated by a finite set  $\Omega \subset R_* \setminus \{0\}$ . Let  $S_W$  be an *Ore closure* of  $\mathcal{M}(\Omega)$  in  $R_*$ , that is a set, containing  $\mathcal{M}(\Omega)$ , which is an Ore set in  $R_*$ . Such a closure always exists since  $R$  is a localization of  $R_*$  with respect to  $S = A_* \setminus \{0\}$ , but we are interested in computing a closure, which is minimal in the sense that there exists no closure  $S'$  satisfying  $\mathcal{M}(\Omega) \subsetneq S' \subsetneq S_W$ .

#### 4.2. Ore Closure in Classical Algebras

In order to localize a domain  $R$  with respect to a multiplicatively closed set  $S$ , the latter needs to be a (left and right) Ore set in  $R$ . Thus, we are going to show, how to compute an Ore closure of  $S$  in  $R$ . Moreover, we ask for small generating sets of a monoidal localization.

Let us recall the well-known Lemma (see e. g. Zariski and Samuel (1975)) first.

**Lemma 4.2.** Let  $f \in K[x] := K[x_1, \dots, x_n]$  be a non-constant monic polynomial and  $S = \{f^i \mid i \in \mathbb{N}_0\}$ . Moreover, let  $f = f_1^{d_1} \cdots f_r^{d_r}$  be an irreducible factorization in  $K[x]$  and  $T := \{f_1^{\alpha_1}, \dots, f_r^{\alpha_r} \mid \alpha \in \mathbb{N}_0^r\}$ . Then  $S^{-1}K[x] = T^{-1}K[x]$ .

Thus, if  $f = (x+1)^2 y^3$ , then  $S = \{(x+1)^{2i} y^{3i} \mid i \in \mathbb{N}_0\}$  and  $T = \{(x+1)^i, y^i \mid i \in \mathbb{N}_0\}$ .

Let  $S$  be a multiplicatively closed subset of a domain  $R$  and  $0 \notin S$ . In order to prove, that  $S$  is an Ore set in  $R$ , one has to show, that  $\forall (s, r) \in S \times R$ , there exist  $(t, q) \in S \times R$ , such that  $r \cdot t = s \cdot q$  in  $R$  and  $\forall (t, q) \in S \times R$  there exist  $(s, r) \in S \times R$ , satisfying the same condition. In other words, one can rewrite any left (resp. right) fraction as a right (resp. left) fraction.

We will analyze the smallest nontrivial Ore sets in the first Weyl, shift and  $q$ -commutative algebras (these results seem to be folklore) and give simple constructive proofs of the Ore property for them.

**Lemma 4.3.** Let  $A_1$  be the first Weyl algebra and  $f \in K[x] \setminus K$ . Then  $S = \{f^i \mid i \in \mathbb{N}_0\}$  is an Ore set in  $A_1$ .

*Proof.* We have for  $f^{i+1}$  and  $i \in \mathbb{N}$ , that  $d \cdot f^{i+1} = f^i \cdot (f d + (i+1) \frac{df}{dx})$ . By induction, one can prove, that for  $j \in \mathbb{N}$  and  $i+1 \geq j$  one has  $d^j \cdot f^{i+1} = f^{i-j+1} \cdot (f^j d^j + v_{ij})$ , where the terms of  $v_{ij} \in A_1$  have degree at most  $j-1$  and contain derivatives up to  $f^{(j)}$ . Suppose we are given  $g = \sum_{j=0}^d b_j(x) d^j \in A_1$  with  $b_d \neq 0$  and  $f^k$  for a fixed  $k \in \mathbb{N}$ . Then

$$d^j \cdot f^{d+k} = d^j \cdot f^{j+k} \cdot f^{d-j} = f^k (f^j d^j + v_{j+k,j}) f^{d-j}$$

Thus

$$g \cdot f^{d+k} = \sum_{j=0}^d b_j(x) d^j \cdot f^{d+k} = f^k \cdot \sum_{j=0}^d b_j(x) (f^j d^j + v_{j+k,j}) f^{d-j}.$$

□

Consider now the first shift algebra  $S_1$  (cf. Example 3.15). Since  $sx = (x+1)s$ , we see that for all  $z \in \mathbb{Z}$

$$(x+z+1)^{-1} s = s(x+z)^{-1}$$

thus it seems natural to have polynomials with integer shifts of their argument in the set  $S$  as above in addition to  $S$  itself.

**Remark 4.4.** For  $f \in K[x] \setminus K$ , the set  $S = \{f^i \mid i \in \mathbb{N}\}$  is not an Ore set in the first shift algebra. Take  $s$  and  $f^k(x) \in S$ , we're looking for  $f^\ell(x)$  and  $t \in S_1$ , such that  $s f^\ell(x) = f^k(x) t$ . The left hand side is  $f(x+1)^\ell s$  thus  $f^k(x) t = f(x+1)^\ell s$ . But  $f(x) \nmid f(x+1)$  for non-constant  $f$ , thus there exists no  $t \in S_1$  satisfying the latter identity. It means, that we have to enlarge  $S$  in order to obtain an Ore set in  $S_1$ .

**Lemma 4.5.** Let  $S_1$  be the first shift algebra (cf. Example 3.15) and  $f \in K[x] \setminus K$ . Then  $S = \{f^n(x \pm z) \mid n, z \in \mathbb{N}_0\}$  is an Ore set in  $S_1$ .

*Proof.* Given  $g = \sum_{j=0}^d b_j(x) s^j \in S_1$  with  $b_d \neq 0$  and  $h(x) = f^k(x+z_0) \in S$  with  $k \in \mathbb{N}, z_0 \in \mathbb{Z}$ , let us define  $g_f(x) := \prod_{i=0}^d h(x-i) \in S$ . Then

$$g \cdot g_f(x) = \sum_{j=0}^d b_j(x) s^j \cdot \prod_{i=0}^d h(x-i) = h(x)^d \cdot \sum_{j=0}^d b_j(x) \left( \prod_{i=0, i \neq j}^d h(x+j-i) s^j \right).$$

□

A similar phenomenon can be observed in quantum algebras as well.

**Lemma 4.6.** Let  $Q_1$  be the first  $q$ -commutative algebra  $K(q)\langle x, s \mid yx = qxy \rangle$  and  $f \in K[x] \setminus K$ . Then  $S = \{f^n(q^{\pm z}x) \mid n, z \in \mathbb{N}_0\}$  is an Ore set in  $Q_1$ .

*Proof.* Note, that for any  $g(x) \in K[x]$  one has  $y^m g(x) = g(q^m x)y$ . Suppose we are given  $g = \sum_{j=0}^d b_j(x)y^j \in Q_1$  and  $h(x) = f^k(q^\ell x) \in S_1$ . Let us define  $g_f(x) := \prod_{i=0}^d h(q^{-i}x) \in S$ . Then

$$g \cdot g_f(x) = \sum_{j=0}^d b_j(x)y^j \cdot \prod_{i=0}^d h(q^{-i}x) = h(x) \cdot \sum_{j=0}^d b_j(x) \prod_{i=0, i \neq j}^d h(q^{j-i}x)y^j.$$

□

Let  $R'$  be a  $K$ -algebra with  $R_* \subseteq R' \subseteq R$ , where  $R_*, R$  are as above and  $M \in R^{m \times m}$ . Consider a system of equations  $M\omega = 0$  in unknown functions  $\omega = (\omega_1, \dots, \omega_m)$  from a space of functions  $\mathcal{F}$ , which will possess some module structure, see below. Assume, that we have computed  $U, V$  (unimodular over  $R$ ) and  $D = \text{Diag}(d_{11}, \dots, d_{mm})$  satisfying  $UMV = D$ .

#### 4.3. $\mathcal{F}$ is an $R$ -module

Inverting  $V$ , we obtain  $UM = DV^{-1}$ , hence  $M\omega = 0$  is equivalent to  $0 = UM\omega = DV^{-1}\omega$ . Thus, introducing an  $R$ -automorphism of  $\mathcal{F}$ , defined by  $\varpi := V^{-1}\omega$ , we obtain a decoupled system  $\{d_{ii}\varpi_i = 0\}$ . Note that if  $d_{ii} = 0$ , then  $\varpi_i$  is called a free variable of the system, e. g. in (Zerz, 2006). The solutions of the decoupled system in  $\mathcal{F}$  are precisely the solutions of  $M\omega = 0$  in  $\mathcal{F}$ .

#### 4.4. $\mathcal{F}$ is an $R_*$ -module

Indeed, the  $R$ -automorphism of  $\mathcal{F}$  above can be defined as soon as  $V$  is invertible. We can regard this as a kind of “analytic” transformation of  $\mathcal{F}$ .

**Proposition 4.7.** Let  $UMV = D$  as before. Let  $S_U$  and  $S_V$  be Ore multiplicative closures of  $U$  and  $V$  respectively, according to Sect. 4.1. Moreover, let  $S$  be an Ore multiplicative closure of the monoid  $S_V \cup S_U$ . Then, over  $S^{-1}R_* \subset R$  we have  $M\omega = 0 \Leftrightarrow D(V^{-1}\omega) = 0$ . Thus it is possible to decouple the system  $M$ . Moreover, there might be solutions in an  $S^{-1}R_*$ -module  $\mathcal{G}$ .

*Proof.* Let  $R_V = (S_V)^{-1}R_*$ . Then on an  $R_V$ -module  $\mathcal{G}$  we can define an  $R_V$ -automorphism  $\omega \mapsto V^{-1}\omega$ . Thus over  $R_V$  we have  $UM\omega = 0 \Leftrightarrow D\varpi = 0$ . Moreover,  $U$  is invertible over  $(S_U)^{-1}R_*$ . Hence, over  $S^{-1}R_*$  we have  $M\omega = 0 \Leftrightarrow UM\omega = 0 \Leftrightarrow D\varpi = 0$ . □

**Corollary 4.8.** With notations of the Proposition, there is an explicit isomorphism of  $S^{-1}R$ -modules

$$(S^{-1}R)^m / (S^{-1}R)^n M \cong (S^{-1}R)^m / (S^{-1}R)^n UMV = (S^{-1}R)^m / (S^{-1}R)^n D.$$

Note that the left transformation matrix  $U$  also can contain essential information about the so-called singularities of a system, which often are connected to meromorphic (and non-holomorphic) solutions.

**Example 4.9.** Over the first Weyl algebra  $A_1 = R_*$ , consider the single equation  $(x d)\omega = 0$ . Here  $U = x$  and thus  $S_U = \{x^i \mid i \in \mathbb{N}_0\}$ . So  $R_U = (S_U)^{-1}R_* \cong K[x, x^{-1}]\langle d \rangle \subsetneq K(x)\langle d \rangle$  and over  $R_U$ , the equation is equivalent to  $d\omega = 0$ , whose solutions in any nonzero  $R$ -module  $\mathcal{F}$  contain  $K$ .

On the other hand, the division by  $x$  over  $R_*$  is not allowed. Consider an  $R_*$ -module  $\mathcal{D}'(\mathbb{R})$  of distributions. Then, we see that a  $K$ -multiple of the Heaviside step function is a solution. Thus,  $K \cdot H(x) \oplus K$  is a subspace of solutions of the system  $(x d)\omega = 0$ .

**Example 4.10.** Consider the univariate sequence space  $\mathcal{S}$ , that is the  $K$ -vector space of all functions  $f : \mathbb{Z} \rightarrow K$ , which is an  $S_1(K)$ -module. Recall, that a discrete analogue  $H(n)$  of the Heaviside step function is defined to be 0, if  $n < 0$  and 1 otherwise.

Consider the analogon of the equation above  $(n(s-1))\omega = 0$  over the shift algebra  $S_1(K) = R_*$ , cf. Example 3.15, where  $s$  acts as  $(s\omega)(n) = \omega(n+1)$ . The invertibility of  $n$  is reflected in the localization with respect to  $\{(n \pm k)^m \mid k, m \in \mathbb{N}_0\}$  (cf. Lemma 4.5) and implies that there is 1-dimensional subspace of constant solutions.

Over  $R_*$ ,  $n$  is not invertible. Moreover, the ideal  $\langle n \rangle \subset R_*$  annihilates any constant multiple of the Kronecker delta  $\delta_{n,0} \in \mathcal{S}$ . Since  $\delta_{n,0} = H(n) - H(n-1) = (s-1)(H(n-1))$ , another set of solutions to the considered equation are  $K$ -multiples of  $H(n-1)$ . Hence, as one can easily check,  $K \cdot H(n-1) \oplus K \subset \mathcal{S}$  is indeed the whole set of solutions to the equation  $(n(s-1))\omega = 0$ .

## 5. Cyclic Vector Method

The existence of the Jacobson form of a matrix over a simple Euclidean domain (Cohn, 1971; Jacobson, 1943) is a very strong result. In particular, for a square matrix  $M$  of full rank over  $R$ , a Jacobson form is  $\text{Diag}(1, \dots, 1, r)$  for some  $r \in R \setminus \{0\}$ . Then a module, presented by  $M$  is isomorphic to a cyclic module and its presentation is a principal ideal. The method of finding a cyclic vector in a finitely presented module and obtaining a left annihilating ideal for it is also used in  $D$ -module theory.

**Proposition 5.1.** Let  $R$  be a simple OLGAED, representable as  $A[d; \sigma, \delta]$  with a division ring  $A$  over the field  $K$ . Let  $M = \text{Diag}(m_1, \dots, m_r)$  be a full rank  $r \times r$  matrix, that is  $m_i \neq 0$ . Then  $d := d(M) = \sum \deg(m_i)$  is an invariant of the module  $R^r/R^r M$ , since it is the dimension of the module over the division ring  $A$ . Let  $p = [p_1, \dots, p_r]^T \in R^{r \times 1}$  and  $c \in R$  be a generator of the left annihilator ideal of  $p$  in the module  $R^r/R^r M$ . If  $\deg(c) = \sum \deg(m_i)$ , then  $\text{Diag}(1, \dots, 1, c)$  is a Jacobson form of  $M$ .

*Proof.* There is an  $R$ -module homomorphism  $\varphi_p$  and the corresponding induced exact sequence

$$0 \longrightarrow R/\langle c \rangle = R/\ker \varphi_p \xrightarrow{-p} R^r/R^r M \longrightarrow \text{coker } \varphi_p \longrightarrow 0.$$

Since all  $R$ -modules above are finite dimensional over  $A$ , the dimension of  $\text{coker } \varphi_p$  is precisely  $d - \deg(c)$ . Hence if  $\deg(c) = d$ , then

$$R^r/R^r \text{Diag}(1, \dots, 1, c) \cong R/\langle c \rangle \cong R^r/R^r M = R^r/R^r \text{Diag}(m_1, \dots, m_r).$$

□

**Remark 5.2.** By using the previous Proposition, we propose the following probabilistic approach for the computation of a cyclic presentation of a module. We use the dimension  $d$  of  $M$  as the certificate. For every  $1 \leq i \leq r$ , consider a polynomial  $p_i$  of degree at most  $\deg(m_i) - 1$  in  $\mathbf{d}$  with random coefficients from  $A$ . Compute the generator  $c \in R$  of  $\ker \varphi_p$ . If  $\deg c = d$ , we are done. Otherwise (it means that the image of  $\varphi_p$  is a proper submodule) one takes another set of random polynomials  $p_i$  and repeats the procedure. In order to turn this approach into an algorithm, one needs to obtain probabilistic estimations on the length of random coefficients like in (Kaltofen et al., 1989) and (Storjohann and Labahn, 1997). However, it is more complicated in the case when  $A$  is non-commutative division ring and needs to be investigated in more detail. Our experiments, illustrated by the examples below, detect a considerable coefficient swell both in the intermediate computations and in the output. Thus we conclude, that the deterministic method by Leykin (Leykin, 2003) is better for the case, when random vectors contain polynomials from  $K[x]$  as coefficients.

Yet another application of this approach is the search for a proper submodule of a module. Namely, if  $\deg c < d$ , the image of  $\varphi_p$  is such a submodule.

In the following examples we work in the first rational Weyl algebra  $A$ . Consider two  $3 \times 3$  diagonal matrices with polynomials of degrees 1, 2, 3 in  $\mathbf{d}$  at the diagonal. We call these matrices  $M_1$  and  $M_2$ . By the remark above, in order to find a cyclic vector of the corresponding module, it is enough to consider a vector  $p$  of the form  $[c(x), a(x)\mathbf{d} + b(x), u(x)\mathbf{d}^2 + v(x)\mathbf{d} + w(x)]^T$  for  $a, b, c, u, v, w \in K[x]$ . We generate the latter polynomials in a random way, taking their coefficients from  $\mathbb{Q}$  from the range  $[0, \dots, 100]$ . The vector  $p_1$  has coefficients of  $x$ -degree at most 3 and the vector  $p_2$  of  $x$ -degree at most 4:

$$\begin{aligned} p_1 &= [98x^3 + 4, (2x^2 + 17)\mathbf{d} + 87x^3, (98x^2 + 11x)\mathbf{d}^2 + (8x^3 + 62x^2 + 31)\mathbf{d} + 89x]^T, \\ p_2 &= [50x^4 + 13x^3 + 97x^2, (25x^4 + 91x + 72)\mathbf{d} + 53x^4 + 96x^3 + 90x, (41x^3 + 57x^2)\mathbf{d}^2 + (36x^4 + 53x^2 + 54x + 83)\mathbf{d} + 2x^3 + 87]^T. \end{aligned}$$

By computing kernels as in Prop. 5.1 we obtain generators  $c_1^i, c_2^i$  for  $i = 1, 2$  respectively. Since  $\deg c_j^i = 6 = \sum_{k=1}^3 \deg M_{kk}$ , it follows that  $p_j$  are cyclic vectors for both matrices  $M_1, M_2$  and the Jacobson form of  $M_i$  with respect to  $p_j$  is  $\text{Diag}(1, 1, c_j^i)$ .

**Example 5.3.** Consider the matrix  $M_1 = \text{Diag}(\mathbf{d}, x\mathbf{d}^2 + 2\mathbf{d}, x^2\mathbf{d}^3 + 4x\mathbf{d}^2 + 2\mathbf{d})$ . For the vector  $p_1$  we obtain the cyclic generator  $c_1^1 = (1011752x^8 - 348435x^7 - 846320x^5 - 2965480x^4)\mathbf{d}^6 + (9105768x^7 - 3484350x^6 - 10155840x^4 - 38551240x^3)\mathbf{d}^5 + (15176280x^6 - 6271830x^5 - 25389600x^3 - 115653720x^2)\mathbf{d}^4 - 35585760x\mathbf{d}^3 + 35585760\mathbf{d}^2$ .

For the vector  $p_2$

$$\text{we obtain the cyclic generator } c_2^1 = (395647200x^{16} - 264348000x^{15} + 72499244880x^{14} - 432343555560x^{13} + 267049574380x^{12} + 8987298499008x^{11} - 45076322620512x^{10} + 91959270441432x^9 - 24315286945590x^8 + 20084358713472x^7 - 19034034270714x^6 - 3963517931016x^5 + 240924562515x^4 + 239689051938x^3)\mathbf{d}^6 + \dots$$

**Example 5.4.** Consider the matrix  $M_2 = \text{Diag}(\mathbf{d}, x\mathbf{d}^2 + 2\mathbf{d}, x^2\mathbf{d}^3 + 3x\mathbf{d}^2 + \mathbf{d})$ . For the vector  $p_1$  we obtain the cyclic generator  $c_1^2 = (8352x^{12} + 149292x^{11} + 3213954x^{10} - 8623701x^9 + 46759968x^8 + 18251056x^7 + 12525848x^6 + 1085484x^5 + 968320x^4)\mathbf{d}^6 + \dots$

For the vector  $p_2$  we obtain the cyclic generator  $c_2^2 = (544946x^{21} - 8586000x^{20} + 4018843296x^{19} - 2355826816422x^{18} + 7580096636636x^{17} - 91394273346228x^{16} + 394488979119486x^{15} - 1039358677414560x^{14} + 2049350822715951x^{13} - 6702303668155704x^{12} + 15453420608607570x^{11} - 9398963461913820x^{10} - 1453404219438726x^9 -$



$$83615730159492x^8 + 313903596685743x^7 + 646008054793470x^6 + 64626268386222x^5 - 13528366907400x^4 - 3553905268080x^3) d^6 + \dots$$

**Analysis of the data.** Since the computed cyclic generators  $c_j^i$  are fraction-free, we present them as polynomials from  $\mathbb{Z}[x, d]$ . We determine the following data and put them into the table.

- NT number of terms, TD total degree;
- BC, SC and AC stand for the biggest resp. the smallest resp. the arithmetic average of absolute values of coefficients;
- BX, SX and AX stand for the biggest resp. the smallest resp. the arithmetic average of degrees in  $x$  in every monomial  $x^a d^b$ .

Poly	NT	TD	BC	SC	AC	BX	SX	AX
$c_1^1$	14	14	$1.15 \cdot 10^8$	$3.48 \cdot 10^5$	$2.14 \cdot 10^7$	8	0	4.3
$c_2^1$	85	22	$3.2 \cdot 10^{15}$	$2.6 \cdot 10^8$	$2.3 \cdot 10^{14}$	16	0	6.8
$c_1^2$	43	18	$3.9 \cdot 10^8$	$8.3 \cdot 10^3$	$6 \cdot 10^7$	12	0	5.8
$c_2^2$	126	27	$4.95 \cdot 10^{17}$	$5.4 \cdot 10^5$	$2.35 \cdot 10^{16}$	21	0	9.4

Let us see, what can happen when the random polynomial coefficients from above are taken to be just numbers from  $K$ .

**Example 5.5.** For the matrix  $M_2$ , let us take 5- and 10-digit random integers. The corresponding vectors are then  $p_1 = [5535, 3892d + 20690, 6069d^2 + 20660d + 17323]^T$  and  $p_2 = [1109725034, 618308146d + 1684065511, 2034108815d^2 + 1702526110d + 1361184996]^T$ . The corresponding cyclic generators are then  $c_1 = (519739491811x^{10} + \dots)d^4 + \dots$  and  $c_2 = (689281531286620056404507706x^{10} + \dots)d^4 + \dots$ .

The coefficient data is put into the table with the same notations as before.

Poly	NT	TD	BC	SC	AC	BX	SX	AX
$c_1$	20	14	$2.14 \cdot 10^{13}$	$4.77 \cdot 10^{10}$	$5.48 \cdot 10^{12}$	10	3	6.5
$c_2$	20	14	$6.15 \cdot 10^{29}$	$6.89 \cdot 10^{26}$	$8.29 \cdot 10^{28}$	10	3	6.5

As we can see from the degree in  $d$ , both  $c_1, c_2$  are not cyclic vectors. Notably, numerous experiments in the setup of this example never led us to a cyclic vector for  $A^3/A^3M_2$ . Instead we repeatedly obtained polynomials  $c_i$  of degree 4. This shows, that there is a 4-dimensional submodule  $N$  of the 6-dimensional module  $A^3/A^3M_2$ , which dominates over others for the special choice of the form of test vectors.

## 6. Normal Form over a General Domain

As we have noted, there are many different-looking normal forms over a non-simple domain.

**Definition 6.1.** Let  $R$  be a ring. An element  $r \in R$  is called **two-sided**, if  $r$  is not a divisor of zero and  ${}_R\langle r \rangle = \langle r \rangle_R$ . It is called **proper**, if  ${}_R\langle r \rangle \subsetneq R$ .

Though in Cohn (1971) a two-sided element has been called **invariant**, we propose to use *two-sided* instead, due to the ubiquity of the word *invariant*.

Let  $R$  be a domain and a  $K$ -algebra. Then  $r \in R$  is proper two-sided if and only if  $\forall s, s' \in R \exists t, t' \in R$  such that  $rs = tr$  and  $s'r = rt'$ . If  $R$  admits a Gröbner basis theory, this is the same as to say “ $\{r\}$  is a two-sided Gröbner basis of the two-sided ideal  $\langle r \rangle$ ”. It is straightforward, that for a simple domain 0 is the only proper two-sided element.

Generalizing the statement in the Example 4.4 of (Levandovskyy and Schindelar, 2011) leads to the following result.

**Lemma 6.2.** Let  $R$  be a non-simple Euclidean domain and a  $K$ -algebra. Moreover, let  $m \leq n$  be natural numbers and  $r \in R$  be a proper two-sided element. Then for the  $2 \times 2$  matrices  $D_1 = \text{Diag}(r^m, r^n)$  and  $D_2 = \text{Diag}(1, r^{m+n})$  the corresponding modules  $M_1 = R^2/R^2D_1$  and  $M_2 = R^2/R^2D_2$  are not isomorphic.

*Proof.* At first, we note that the set of proper two-sided elements is multiplicatively closed, thus  $r^n, r^m, r^{n+m}$  are proper two-sided. As we can see,  $\text{Ann}_R M_2 = \langle r^{m+n} \rangle$  and  $\text{Ann}_R M_1 = \text{Ann}_R(R/\langle r^m \rangle \oplus R/\langle r^n \rangle) = \langle r^m \rangle \cap \langle r^n \rangle = \langle r^n \rangle$ . We have to show that the two-sided ideals  $\text{Ann}_R M_1, \text{Ann}_R M_2$  are not equal, then the claim follows. Let  $S = R \otimes_K R^{opp}$  be the enveloping algebra of  $R$  and  $\iota : R \rightarrow S$  a natural embedding of  $K$ -algebras, then any two-sided ideal of  $R$  is a left ideal over  $S$ . Suppose that for two-sided ideals  $\langle r^n \rangle \subseteq \langle r^{m+n} \rangle$ . Over  $S$  we have the inequality of left ideals  $\langle \iota(r^n) \rangle \subseteq \langle \iota(r^{m+n}) \rangle$ , hence there exists  $s \in S$ , such that  $\iota(r^n) = s\iota(r^{m+n}) = s\iota(r^m)\iota(r^n)$ . Then  $(s\iota(r^m) - 1) \cdot \iota(r^n) = 0$  and hence  $s\iota(r^m) = 1$ , since  $S$  is a domain. Thus,  $\langle \iota(r^m) \rangle = S$  as a left ideal and hence  $\langle r^m \rangle = R$ , what is a contradiction to the assumption that  $r$  is a proper two-sided element.  $\square$

Recall that for  $a, b \in R$ , one says that  $a$  totally divides  $b$  (and denotes  $a \parallel b$ ) if and only if there exists a two-sided  $c \in R$ , such that  $a \mid c \mid b^5$  (Cohn, 1971). Moreover,  $a \parallel a$  if and only if  $a$  is two-sided element.

**Example 6.3.** In the first shift algebra  $R_* = S_1$ , cf. Example 3.15, consider the diagonal matrices

$$D_1 = \begin{bmatrix} s+x & 0 \\ 0 & s(s+x) \end{bmatrix} \quad \text{and} \quad D_2 = \begin{bmatrix} s & 0 \\ 0 & s(s+x) \end{bmatrix}.$$

At first, let us analyze the appearing elements for the proper two-sidedness. By computing two-sided Gröbner bases over  $S_1$ , we obtain that  $s$  is already such a basis, whereas  $s_1\langle s+x \rangle_{S_1} = s_1\langle x, s \rangle_{S_1}$  and  $s_1\langle s(s+x) \rangle_{S_1} = s_1\langle (x+1)s, s^2 \rangle_{S_1}$ . Thus neither  $s+x$  nor  $s(s+x)$  are proper two-sided in  $R_*$ . In the localization  $R = (K[x] \setminus \{0\})^{-1}R_*$ , we even see that  ${}_R\langle s+x \rangle_R = R$  and  ${}_R\langle s(s+x) \rangle_R = R\langle s \rangle_R$ .

In the matrix  $D_2$  there is a total divisibility on the diagonal. Indeed,  $s$  is proper two-sided and  $s \mid s(s+x)$ . Hence, for any  $f \in R$  the result of reduction of  $s$  with  $fs(s+x) = f(s+x+1)s$  will be  $(1-f(s+x+1))s \in \langle s \rangle$ . Hence, no reduction procedure will lead to a unit instead of  $s$ .

<sup>5</sup> Recall, that  $a \mid c$  if  $\exists d \in R$  such that either  $c = ad$  or  $c = da$  holds.

On the other hand, we see that  $s(s+x) \in \langle s \rangle$ . Then  $s(s+x) - fs = (s+x+1-f)s$  has degree 1 in  $s$  only for  $f = s - g(x)$ , where  $g(x) \neq -(x+1)$ . This reduction produces  $[0, s(s+x)]^T - (s - g(x)) \cdot [s, s]^T = [-(s - g(x))s, (g(x) + x + 1)s]^T$ , which does not lower the degree in the column but only interchanges terms of degrees 1 and 2. Hence no further essential simplification is possible, since replacing  $s(s+x)$  by a similar factor can neither lower the degree nor lead to a two-sided element.

In the matrix  $D_1$ , there is no total divisibility on the diagonal, hence we will be able to achieve the lower degree. And indeed, for

$$U = \begin{bmatrix} 1 & 1 \\ s^2 + xs + 2s & s^2 + xs + 2s + x + 2 \end{bmatrix}, \quad V = \begin{bmatrix} s + 1 & -s^2 - xs - s \\ -1 & s + x - 1 \end{bmatrix}$$

which are  $R$ -unimodular, we obtain that

$$UD_1V = \begin{bmatrix} x & 0 \\ 0 & x + 2 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & s(s+x)(s+x-1) \end{bmatrix}.$$

Thus  $D_1$  possesses even the Jacobson normal form  $\text{Diag}(1, s(s+x)(s+x-1))$  over  $R$ .

## 7. Implementation and Examples

Our implementation of the computation of a diagonal form together with transformation matrices is called `jacobson.lib`. It is distributed together with SINGULAR (Decker et al., 2011) since its version 3-1-0. In the Appendix we put an example of a SINGULAR session with input, output and explanations.

### 7.1. Comparison

There are other packages to compute diagonal and Jacobson forms. The package JANET for MAPLE (Blinkov et al., 2003; Chyzak et al., 2007) directly follows the classical algorithm with no special optimizations. In MAPLE packages by H. Cheng et al. (Beckermann et al., 2006; Cheng and Labahn, 2007; Davies et al., 2008) modular (MODREDUCE) and fraction-free (FFREDUCE) versions of an order basis of a polynomial matrix  $M$  from an Ore algebra  $A$  are implemented. The computation of the left nullspace of  $M$  and indirectly the Popov form of  $M$  uses order bases. There are also experimental implementations, mentioned in (Culianez and Quadrat, 2005) and (Middeke, 2008).

In (Levandovskyy and Schindelar, 2011), we compared our implementation with the one by D. Robertz. It turned out that with our implementation, one experiences moderate swell of coefficients and obtains uncomplicated transformation matrices.

Unlike in theoretical considerations, our implementation usually returns diagonal matrices with elements of descending degrees on the main diagonal.

### 7.2. Examples

**Example 7.1.** Consider two versions of the Example 3.8 in (Levandovskyy and Schindelar, 2011).

(A). In the first Weyl algebra  $R_* = K[x][\partial; \text{id}, \frac{d}{dx}]$ , consider the matrix

$$M = \begin{bmatrix} \partial^2 - 1 & \partial + 1 \\ \partial^2 + 1 & \partial - x \end{bmatrix} \in R^{2 \times 2}.$$

Then the algorithm computes

$$UMV = \begin{bmatrix} (x+1)^2 \partial^2 + 2(x+1)\partial - (x^2+1) & 0 \\ 0 & 1 \end{bmatrix} = D,$$

$$U = \begin{bmatrix} -(x+1)\partial + x^2 + x + 1 & (x+1)\partial + x \\ \partial - x & -\partial - 1 \end{bmatrix}, \quad V = \begin{bmatrix} 1 & 0 \\ (x+1)\partial^2 + 2\partial - x + 1 & 1 \end{bmatrix}.$$

Let us analyze the transformation matrices for  $R_*$ -unimodularity. Indeed,  $V$  is unimodular over  $R_*$  since it admits an inverse  $V'$ . However,  $U$  is unimodular over  $S^{-1}R_*$  for  $S = \{(x+1)^i \mid i \in \mathbb{N}_0\}$  (cf. Lemma 4.3) since  $U \cdot Z = W$  and  $W$  is invertible in the ring containing the inverse of  $(x+1)^2$ , that is over a ring, containing  $S^{-1}R_*$ .

$$V' = \begin{bmatrix} 1 & 0 \\ -(x+1)d^2 - 2d + x - 1 & 1 \end{bmatrix}, \quad Z = \begin{bmatrix} 2(d+1) & (x+1)d + x - 2 \\ 2(d-x) & (x+1)d - x^2 - x - 3 \end{bmatrix}, \quad W = \begin{bmatrix} 0 & -4(x+1)^2 \\ 2 & 5(x+1) \end{bmatrix}.$$

(B). In the first shift algebra  $S_1$ , cf. Example 3.15, one has

$$\text{Diag}((x+1)(x+2)s^2 + 2(x+1)s - (x-1)(x+2), 1) = \begin{bmatrix} -(x+1)s + x(x+2) & (x+1)s + x + 2 \\ -s + x + 1 & s + 1 \end{bmatrix} \cdot \begin{bmatrix} s^2 - 1 & s + 1 \\ s^2 + 1 & s - x \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ -(x+2)s^2 - 2s + x & 1 \end{bmatrix}.$$

Denote the equality above as  $D = UMV$ , it turns out, that  $V$  is even  $R_*$ -unimodular.  $U$  becomes invertible in a localization, containing  $(x+2)^{-1}$ , thus, by Lemma 4.5, containing a ring  $S^{-1}R_*$  for  $S = \{(x \pm n)^m \mid n, m \in \mathbb{N}_0\}$ .

**Example 7.2.** Consider now the same matrix as in Example 3.15 over the first Weyl algebra  $R_* = K\langle x, d \mid dx = x d + 1 \rangle$ , respectively  $R = K(x)\langle d \mid dx = x d + 1 \rangle$ :

$$M = \begin{bmatrix} (x-1)d + x^2 - x & x d + x^2 & (x+2)d + x^2 + 2x \\ d + x & 0 & d \end{bmatrix}.$$

We obtain

$$D = \begin{bmatrix} 0 & 3x^2(x+2)^2 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad U = \frac{1}{2} \begin{bmatrix} x(x+2)d - 2(x+1) & -x(x+2)^2 d - (x^4 + 4x^3 + 3x^2 - 4x - 4) \\ (x+1)d - 2 & -(x+1)(x+2)d - (x^3 + 3x^2 + x - 3) \end{bmatrix},$$

$$V = \begin{bmatrix} -(x^4 - 9x^2)d^2 - (x^5 - x^3 - 18x)d - (6x^4 - 24x^2 + 18) & v_{12} & 0 \\ -(3x^3 - 27x)d^2 - (x^5 + 5x^4 - 9x^3 - 18x^2 - 81)d - (x^6 + 2x^5 - 6x^4 + 8x^3 + 9x^2 - 54x) & v_{22} & 0 \\ (x^4 - 9x^2)d^2 + (2x^5 - 10x^3 - 18x)d + (x^6 - 15x^2 + 18) & v_{23} & 1 \end{bmatrix},$$

where  $v_{12} = (x^3 + 3x^2 - 2x)d^2 + (x^4 + 3x^3 + 4x^2 + 6x + 2)d + (5x^3 + 12x^2 - 6)$ ,  $v_{22} = (3x^2 + 9x - 6) \cdot d^2 + (x^4 + 8x^3 + 13x^2 + 11x + 27) \cdot d + (x^5 + 5x^4 + 6x^3 + 14x^2 + 42x + 23)$  and  $v_{23} = -(x^3 + 3x^2 - 2x)d^2 - (2x^4 + 6x^3 + 2x^2 + 6x + 2)d - (x^5 + 3x^4 + 8x^3 + 18x^2 + 12x - 6)$ .

$U$  is unimodular in the localization with respect to  $S_U$ , which is generated as monoid by  $x, x+1, x+2$ .  $V$  is unimodular in the localization with respect to  $S_V$ , which is generated

by  $x, x+2, x+3, x-3$ . Thus, the isomorphism of modules lifts from  $R$  to  $S^{-1}R_*$ , where  $S = \{x^{i_1}(x+1)^{i_2}(x+2)^{i_3}(x+3)^{i_4}(x-3)^{i_5} \mid i_j \in \mathbb{N}_0\}$ .

The same system over the shift algebra was computed in detail in Example 3.15. There it turns out, that  $U$  is unimodular over a ring containing  $(x+2)^{-1}$  and  $V$  is unimodular over a ring containing the inverses of  $\{x-2, x-1, x, x+3, x+4\}$ . Due to Lemma 4.5, the needed Ore set for the localization is not smaller than  $S = S_U = S_V = \{(x \pm n)^m \mid n, m \in \mathbb{N}_0\}$ .

## 8. Conclusion, Further Research and Open Problems

### 8.1. Further Research

We do not perform an analysis of the theoretical complexity of our algorithm, since it has been designed by using Gröbner bases, thus the formal complexity is too high. Indeed, one can see, that we use Gröbner bases rather for convenience, that is in order to present an algorithm, working over arbitrary OLGAE. The original (non-fraction-free) algorithm can be reformulated in terms of extended left and right greatest common divisors over a concrete algebra. To the best of our knowledge, the theoretical complexity of such GCD algorithms depends on the given algebra. For rational Weyl algebras over general fields of characteristic zero there is a paper (Grigor'ev, 1990). It is interesting to find estimations for classical operator algebras like the shift algebra,  $q$ -Weyl and  $q$ -commutative algebras with rational coefficients. Having this information, one could perform complexity analysis for the kind of algorithms we propose. It was reported in (Middeke, 2008), that the Jacobson form can be computed in polynomial time. In our opinion this should be formulated more precisely in the framework, proposed in (Grigor'ev, 1990). We do not claim that our algorithm is superior in terms of theoretical complexity to the others but stress, that its fraction-free version is widely applicable in practical computations. In particular, our algorithm returns transformation matrices with reasonable sizes of their entries and their coefficients.

Concerning the further development of our implementation in SINGULAR (Decker et al., 2011) called `jacobson.lib`, we plan the following enhancements. In order to provide diagonal form computations over  $q$ -algebras like  $q$ -commutative,  $q$ -shift,  $q$ -difference and  $q$ -Weyl algebras, we need to find involutive antiautomorphisms. It turns out, that there are no  $K(q)$ -linear but  $K$ -linear involutions, which act on  $q$  as a non-identical involutive automorphism of  $K(q)$ . We will work on finding such involutions and adapt the implementation to the more general situation. Moreover, it is possible to employ modular Gröbner bases in the implementation.

We have demonstrated, how working with a ring  $R_*$  and its localization  $S^{-1}R_*$  with respect to some Ore set  $S \subset R_*$  is used in various situations. In this paper we concentrated on rings of polynomials respectively rational functions. The same ideas in theory immediately apply to operator algebras  $R_* = K[[x]]\langle d \rangle$  and  $R = K((x))\langle d \rangle$ . However, in practical computations with the computer we are restricted to finite power series, presented by a Laurent polynomial.

For the Weyl and  $q$ -Weyl algebras over a field  $K$  with  $\text{char } K = 0$ , algorithmic computations are possible over the local ring  $K[x]_{\mathfrak{m}_p}$  for  $p \in K^n$  and  $\mathfrak{m}_p = \langle x_1 - p_1, \dots, x_n - p_n \rangle$ . Notably, the Ore completion of the set  $K[x] \setminus \{\mathfrak{m}_p\}$  over shift and  $q$ -shift algebras will contain zero. Thus, there is no analogon to the situation with  $(q)$ -Weyl algebras.

## 8.2. Open Problems

1. From the description and the proof of the Algorithm 3.12, we need in principle only the existence of a terminating Gröbner basis algorithm over  $R$  resp.  $R_*$ . The latter relies on the constructivity of basic operations with fractions in  $R$  via  $R_*$ . Thus the Algorithm 3.12 immediately extends to the case of a general OLGA  $(R, B, I)$  (cf. Def. 2.2) for a nontrivial completely prime ideal  $I \subset B$  by Bueso et al. (2003). In which bigger class of algebras one can perform concrete computations? One can work with local rings like  $K[x]_{\mathfrak{m}_p}$ ,  $p \in K^n$  and  $K[[x]]$  for  $\text{char } K = 0$  or with  $K\{x\}$  for  $K = \mathbb{R}, \mathbb{C}$  as coefficient domains.

2. The algorithm computes  $U, V, D$  such that  $UMV = D$ . It is clear, that  $U, V$  are not unique. By fixing  $M$  and  $D$ , how can one describe the set  $\{(U, V) \mid UMV = D\}$ ? Does there exist  $U'$  resp.  $V'$  from this set, such that special properties like unimodularity hold? This is connected, in particular, to the recent results of A. Quadrat and T. Cluzeau (Cluzeau and Quadrat, 2010). Namely, they prove the existence of matrices  $U$  and  $V$ , which are unimodular over  $R_*$  for certain situations and present an algorithm for the computation of these matrices.

3. One of the most important problems in non-commutative computer algebra is to show algorithmically, that two given finitely presented modules are not isomorphic. It is still open even for cyclic modules over general simple Euclidean Ore domain. Namely, let  $R$  be the latter domain and  $a, b \in R$  with  $\deg a = \deg b > 0$ . Up to now there is no algorithm, which determines that  $R/\langle a \rangle \not\cong R/\langle b \rangle$ . However, there are several situations, where this question has been solved.

In Cluzeau and Quadrat (2008), the authors presented a semi-algorithm for finitely presented modules. Given degree bounds for the variables, the algorithm first looks for matrices, determining a homomorphism. If such a pair has been found, the kernel and cokernel of the corresponding homomorphism are computed and returned.

4. As we have seen, over non-simple domains we have many different normal forms. Starting with classical operator algebras like the  $(q-)$ shift algebra and  $q$ -Weyl algebra, it is important to describe possible normal forms.

5. As in the previous item, what is the most probable normal form for a random square matrix (which is then of full rank) over a non-simple domain? Though it seems that this might depend on the algebra, we conjecture the  $\text{Diag}(1, \dots, 1, p)$ , that is a Jacobson form, is the most probable one. Such approach might lead to the classification as in 4.

## Acknowledgments

We express our gratitude to Eva Zerz and Hans Schönemann for discussions and their advice on numerous aspects of the problems, treated in this article. We thank Daniel Robertz, Johannes Middeke and Howard Cheng for explanations about respective implementations. We are grateful to Mark Giesbrecht, George Labahn and Dima Grigoriev for discussions concerning normal forms for matrices and complexity of algorithms. Many thanks to Moulay Barkatou and Sergey Abramov for explanations of their algorithms for linear functional systems. The first author is grateful to the SCIENCE project (Transnational access) at RISC for supporting his visits to RISC and the usage of computational infrastructure at RISC. We would like to thank the anonymous referees, who helped us a lot with their insightful remarks and suggestions. Kristina Schindelar carried out her work on this paper during her Ph.D. studies at Lehrstuhl D für Mathematik of RWTH Aachen University.

## References

- Apel, J., 1988. Gröbnerbasen in nichtkommutativen Algebren und ihre Anwendung. Dissertation, Universität Leipzig.
- Beckermann, B., Cheng, H., Labahn, G., 2006. Fraction-free row reduction of matrices of Ore polynomials. *J. Symbolic Computation* 41 (5), 513–543.
- Blinkov, Y. A., Cid, C. F., Gerdt, V. P., Plesken, W., Robertz, D., 2003. The MAPLE package "janet": II. Linear Partial Differential Equations. In: *Proceedings of the 6th International Workshop on Computer Algebra in Scientific Computing*. pp. 41–54.  
URL <http://wwwb.math.rwth-aachen.de/Janet>
- Bueso, J., Gómez-Torrecillas, J., Verschoren, A., 2003. Algorithmic methods in non-commutative algebra. Applications to quantum groups. Kluwer Academic Publishers.
- Cheng, H., Labahn, G., 2007. Modular computation for matrices of Ore polynomials. In: *Computer Algebra 2006: Latest Advances in Symbolic Algorithms*. pp. 43–66.
- Chyzak, F., Quadrat, A., Robertz, D., 2007. OREMODULES: A symbolic package for the study of multidimensional linear systems. In: Chiasson, J., Loiseau, J.-J. (Eds.), *Applications of Time-Delay Systems*. Springer LNCIS 352, pp. 233–264.  
URL <http://wwwb.math.rwth-aachen.de/OreModules>
- Chyzak, F., Salvy, B., 1998. Non-commutative elimination in Ore algebras proves multivariate identities. *J. Symbolic Computation* 26 (2), 187–227.
- Cluzeau, T., Quadrat, A., 2008. Factoring and decomposing a class of linear functional systems. *Linear Algebra and its Applications* 428 (1), 324 – 381.
- Cluzeau, T., Quadrat, A., 2010. Serre’s reduction of linear partial differential systems with holonomic adjoints. Tech. Rep. 7486, INRIA.
- Cohn, C., 1971. *Free Rings and their Relations*. Academic Press.
- Culianez, G., Quadrat, A., 2005. Formes de Hermite et de Jacobson: implementations et applications. Tech. rep., INRIA Sophia Antipolis.
- Davies, P., Cheng, H., Labahn, G., 2008. Computing Popov form of general Ore polynomial matrices. In: *Proceedings of the Milestones in Computer Algebra (MICA) Conference*. pp. 149–156.
- Decker, W., Greuel, G.-M., Pfister, G., Schönemann, H., 2011. SINGULAR 3-1-3 — A computer algebra system for polynomial computations.  
URL <http://www.singular.uni-kl.de>
- García García, J. I., García Miranda, J., Lobillo, F. J., 2009. Elimination orderings and localization in PBW algebras. *Linear Algebra Appl.* 430 (8-9), 2133–2148.
- Gianni, P., Trager, B., Zacharias, G., 1988. Gröbner bases and primary decomposition of polynomial ideals. *J. Symbolic Computation* 6 (2-3), 149–167.
- Greuel, G.-M., Levandovskyy, V., Motsak, O., Schönemann, H., 2010. PLURAL. A SINGULAR 3-1 Subsystem for Computations with Non-commutative Polynomial Algebras.  
URL <http://www.singular.uni-kl.de>
- Grigor’ev, D., 1990. Complexity of factoring and calculating the GCD of linear ordinary differential operators. *J. Symbolic Computation* 10 (1), 7 – 37.
- Ilchmann, A., Mehrmann, V., 2006. A behavioral approach to time-varying linear systems. I: General theory. *SIAM J. Control Optim.* 44 (5), 1725–1747.
- Ilchmann, A., Nürnberger, I., Schmale, W., 1984. Time-varying polynomial matrix systems. *Int. J. Control* 40, 329–362.

- Insua, M. A., 2005. Varias perspectivas sobre las bases de Gröbner: Forma normal de Smith, Algoritmo de Berlekamp y álgebras de Leibniz. Ph.D. thesis, Universidade de Santiago de Compostela, Spain.
- Jacobson, N., 1943. The Theory of Rings. American Mathematical Society.
- Kaltofen, E., Krishnamoorthy, M. S., Saunders, B. D., 1989. Mr. Smith goes to Las Vegas: Randomized parallel computation of the Smith normal form of polynomial matrices. In: Davenport, J. H. (Ed.), Proc. EUROCAL '87. Vol. 378 of LNCS. Springer, pp. 317–322.
- Kredel, H., 1993. Solvable polynomial rings. Shaker.  
URL <http://krum.rz.uni-mannheim.de/publicatons.html>
- Levandovskyy, V., 2005. Non-commutative computer algebra for polynomial algebras: Gröbner bases, applications and implementation. Ph.D. thesis, Universität Kaiserslautern.  
URL <http://kluedo.ub.uni-kl.de/volltexte/2005/1883/>
- Levandovskyy, V., Schindelar, K., 2011. Computing diagonal form and Jacobson normal form of a matrix using Gröbner bases. J. Symbolic Computation, 46 (5), 595–608.
- Levandovskyy, V., Schönemann, H., 2003. Plural — a computer algebra system for non-commutative polynomial algebras. In: Proc. of the International Symposium on Symbolic and Algebraic Computation (ISSAC'03). ACM Press, pp. 176 – 183.  
URL <http://doi.acm.org/10.1145/860854.860895>
- Leykin, A., 2003. Algorithms in computational algebraic analysis. Ph.D. dissertation, University of Minnesota.  
URL <http://scholar.lib.vt.edu/theses/available/etd-03262004-082608/>
- Lübeck, F., 2002. On the computation of elementary divisors of integer matrices. J. Symbolic Computation 33 (1), 57–65.
- Middeke, J., 2008. A polynomial-time algorithm for the Jacobson form for matrices of differential operators. Tech. Rep. 2008-13, RISC, J. Kepler University Linz.
- Storjohann, A., Labahn, G., 1997. A fast Las Vegas algorithm for computing the Smith normal form of a polynomial matrix. Linear Algebra Appl. 253, 155–173.
- Zariski, O., Samuel, P., 1975. Commutative Algebra. Vol. 1. With the cooperation of I. S. Cohen. 2nd ed. Graduate Texts in Mathematics. 28. Springer-Verlag.
- Zerz, E., 2006. An algebraic analysis approach to linear time-varying systems. IMA J. Math. Control Inf. 23 (1), 113–126.
- Zerz, E., 2007. State representations of time-varying linear systems. In: Park, H., Regensburger, G. (Eds.), Gröbner Bases in Control Theory and Signal Processing. Vol. 3 of Radon Series Comp. Appl. Math. Walter de Gruyter & Co., pp. 235–251.

## 9. Appendix. The Code for an Example

Consider the code for Example 3.15. After starting a SINGULAR session, we need to set up the algebra first.

```
> LIB "jacobson.lib"; // load the library
> ring w = 0,(x,s),(a(0,1),Dp);
```

The ring  $w$  is a commutative one in variables  $x, s$  over the field  $\mathbb{Q}$  (0 stands for the characteristic). The substring  $(a(0,1), Dp)$  defines a monomial ordering on  $w$ , which in this case is an extra weight ordering, assigning weights 0 to  $x$  and 1 to  $s$ . If two monomials are of the same weight, they are further compared with  $Dp$  (degree lexicographic



ordering). The described ordering mimicks the ordering on the rational shift algebra. For computations one can also use other orderings, like `Dp` or `dp`, cf. the SINGULAR manual.

```
> def W=nc_algebra(1,s); // set up shift algebra
> setring W;
```

This code creates and sets active a new ring `W` as a non-commutative ring from `w` with the relation  $s \cdot x = 1 \cdot xs + s$ . By executing `W`; a user will obtain the description of the active ring.

```
> matrix m[2][3]=
>   x*s-s+x^2-x, x*s+x^2, x*s+2*s+x^2+2*x,
>   s+x,0,s;
> list J=jacobson(m,0);
```

Here the matrix was entered and the algorithm called. Note, that putting a string `printlevel=2`; before the `jacobson` call will output the progress of the algorithm. Higher values of `printlevel` will lead to more details printed during the execution. The list `J` has three entries, namely  $U, D, V$ .

```
> print(J[1]*m[J[3]-J[2]]); // check UmV=D
==> 0,0,0,
      0,0,0
> print(J[2]); // that is D
==> 0,x4+3x3-x2-3x,0,
      0,0,          x
> print(J[1]); // that is U
==> 0,  -1/4x2-x-3/4,
      1/4,-1/4x-1/2
> print(J[3]); // that is V
==> _[1,1],_[1,2],xs2-s2+x2s-xs,
      _[2,1],_[2,2],_[2,3],
      _[3,1],_[3,2],_[3,3]
```

The symbols `_[2,2]` before are printed, when the entries are long. One can access them as single polynomials

```
> print(J[3][2,2]);
==> -21s2-7x2s-2xs+11s-3x3-2x2+13x-8
```